macrosine

oobe
a Fujitsu company

The Australian Digital Health Agency is strengthening My Health Record protections. Are you ready?

What's changing and how will it affect my organisation?

The Australian Digital Health Agency has identified a set of security requirements for systems connecting to the My Health Record system comprising of controls related to application hardening (among others), with controls aligned to the Australian Cyber Security Centre's (ACSC) Essential Eight Maturity Model.

Controls SEC-0040 and SEC-0260, both of which address the handling of Microsoft Office macros, are mandatory conformance requirements for the updated My Health Record System Conformance Assessment Scheme (CAS) for connecting systems. If you're not ready for these changes then you may no longer meet the requirements to access or integrate with the My Health Record System.

Why are SEC-0040 and SEC-0260 being mandated?

Threat actors have long since used legitimate applications to infiltrate and laterally move across compromised environments. The reasons for this are clear; the likelihood of being detected is much lower when common applications are leveraged instead of malicious tools that might trigger prevention or detection controls.

With Macrosine you can retain all of the productivity of Microsoft Office macros, achieve the highest possible security maturity level, ensure the lowest business impact, and meet the mandatory requirements set forth by SEC-0040 and SEC-0260.

How does Macrosine work?

- Macrosine's world-class security scanning capability allows you to sandbox, detonate, and validate Microsoft Office macros.
- Upload your Microsoft Office macro-enabled file to the Macrosine server to scan and digitally sign if validated as safe.
- Configure your organisation to only allow the execution of signed macros and scripts, delivering the highest level of assurance.
- Install on your on-premises infrastructure or in your own subscription in Azure.

Why use Macrosine?

- Automate the security assessment and signing process for macros.
- Meet your Microsoft Office macro security requirements for the My Health Record System CAS.
- Enable your business to use the macros and scripts it relies on without compromising security.

For more information, or to see a demo of Macrosine, contact us at **hello@macrosine.com.au**

macrosine

Essential Eight compliance made simple

Eight steps to better cyber security

Cyber threats are a constant reality. The Australian Cyber Security Centre (ACSC) understands this and has taken action by arming us with the Essential Eight1.The Essential Eight is a best-practice framework based on a set of key mitigation strategies that has been widely adopted by government and commercial organisations and is endorsed by the cyber security industry. In some industries and sectors it has been mandated by government policy, while in others, organisations can aim for their own maturity level based on their specific risk appetite.

The Essential Eight defines maturity levels against each strategy ranging from 0 (nothing) to 3 (ideal). Achieving level 3 maturity for each mitigation strategy, whilst ideal, might not always be achievable for some organisations, however, the accepted approach is to decide on an achievable target state and accept the risk that comes with lower maturity levels.

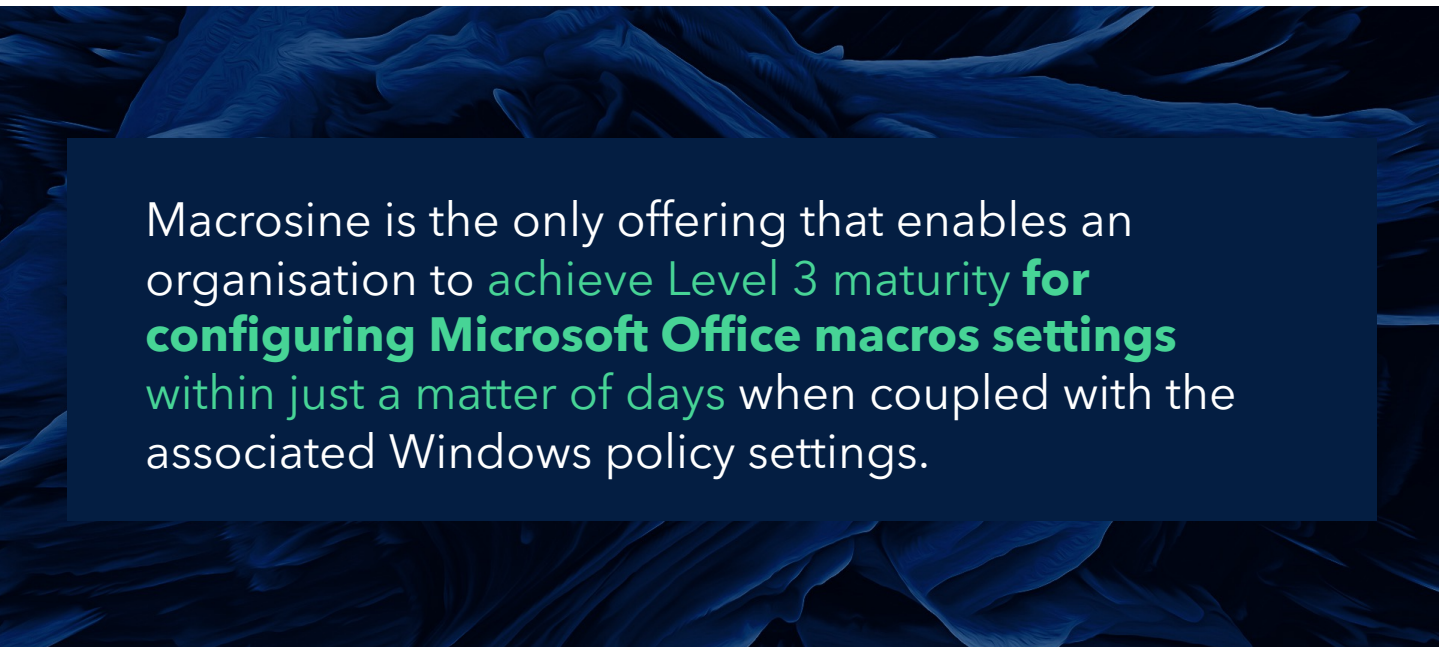
The strategies within the Essential Eight are ...

1 Application control	2 Patch applications	3 Configure Microsoft Office macros settings	4 User application hardening
5 Restrict administration privileges	6 Patch operating systems	7 Multi-factor authentication	8 Regular backups

1 See https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

macrosine

How can Macrosine help?



Macrosine can be installed on a variety of supported platforms, including on-premises infrastructure or Microsoft Azure, allowing users to then upload their macro-enabled Microsoft Office files and PowerShell scripts so they can be security assessed in order to check that they're safe to use.

The assessment executes the files in a sandbox and Macrosine monitors the results. Based on the behaviour of the file in the sandbox a risk rating is applied and the user can then decide which action to take based on this rating –either to quarantine the file or to apply a digital signature aligned to the risk. You then configure all of your Windows devices to only allow the use of digitally signed macro-enabled Microsoft Office files and PowerShell scripts, and the job's done. You've now levelled up to Level 3.

macrosine

Macrosine is licensed annually, on a 1-to-5-year subscription per environment, per company, per country.

oobe
a Fujitsu company

The service is implemented, maintained, and supported by oobe, a Fujitsu company. Any major product updates are applied in co-ordination with the client.

macrosine

Essential Eight and your industry

Implementing any of the mitigation strategies in the ACSC Essential Eight enhances your cyber security posture, regardless of your industry. Some industries and regulatory frameworks, such as AESCSF, ADHA, and the PSPF, actually mandate specific Microsoft Office macro controls.

Australian Digital Health Agency (ADHA)

Security Requirements Conformance Profile 1.0, released for consultation in December 2022 and due to be effective from April 2023, requires all organisations that digitally connect to My Health Record systems to adopt new security practices. This profile specifically mandates Essential Eight Office Macro controls with the ideal aim to adopt Level 3, digitally signed Office Macros.

Australian Energy Sector Cyber Security Framework (AESCSF)

The AESCSF was first developed in 2018 and has since been extended to cover Electricity, Gas and Liquid Fuels sectors, and Version 2 of the AESCSF is due in 2023. Control ACM-2C calls for the configuration of Office Macro settings to only allow vetted macros from trusted locations with limited write access or digitally signed with a trusted certificate.

Australian Protective Security Policy Framework (PSPF)

This is a mandatory policy framework applying to all Australian Government entities and non-corporate Commonwealth entities in Australia and overseas. It implements four core policies for Security Governance, Information Security, Personal Security and Physical Security. Information Security - Policy 10, Safeguarding data from cyber threats, explicitly calls out implementing Essential Eight and Microsoft Office macro mitigation settings.

For more information, check out macrosine.com.au or contact hello@macrosine.com for a personalised client assessment.

macrosine